Федеральное агентство по образованию
Государственное образовательное учреждение
высшего профессионального образования
Ивановский государственный химико-технологический университет

С.С.Алаева, С.П. Бобков, С.В. Ситанов

Администрирование в информационных сетях

Учебное пособие

Иваново 2010

УДК 681.3

Алаева С.С., Бобков, С.П., Ситанов С.В. Администрирование в информационных системах: учеб. пособие / Иван. гос. хим.-технол. ун-т. Иваново, 2010. 52 с.

Учебное пособие посвящено изучению теоретических и практических основ администрирования в информационных системах, способов управления информационными сетями.

Подробно рассмотрены вопросы инсталляции, эксплуатации и сопровождения информационных систем. Большое внимание уделено изучению служб управления: конфигурацией и изменениями; контролем характеристик; ошибочными ситуациями; учетом и безопасностью; планирования и развития. Подробным образом освещены вопросы аудита информационных систем; функции, процедуры администрирования; объекты администрирования; методы администрирования; аппаратно-программные платформы администрирования.

Предназначено для самостоятельной работы студентов, обучающихся по направлению подготовки «Информационные системы и технологии». Кроме того, данный материал может быть полезным для студентов других специальностей и направлений.

Ил. 13. Библиогр.: 5 назв.

Печатается по решению редакционно-издательского совета Ивановского государственного химико-технологического университета.

Рецензенты:

кафедра математики, экономической теории и вычислительной техники Ивановского филиала Российского государственного торгово-экономического университета;

ст. преподаватель кафедры вычислительной и прикладной математики Ивановского государственного университета Д.В. Туртин.

ВВЕДЕНИЕ

В настоящее время специалисты в области «Информационные системы в технике и технологиях» являются одними из наиболее востребованных на международном рынке труда, а среди категорий профессиональных работников в области информационных технологий - одними из наиболее высокооплачиваемых.

Потребность в таких специалистах возникла в связи с возрастающей ролью в современном мире информационных систем. Любая информационная система функционирует на конкретном уровне мирового хозяйства (микро-, мезо-, макро- и мегаэкономики) в муниципальных, государственных, негосударственных и международных организациях различного назначения, в органах управления, министерствах, ведомствах и подчиненных им организациях, в органах юрисдикции, юридических и адвокатских консультациях, судах, правоохранительных органах, экономических, банковских, налоговых учреждениях, учебных заведениях, общественных организациях, в ассоциациях и объединениях, на предприятиях различной организационно-правовой формы, в органах охраны природы, распределения природных ресурсов и энергоносителей, в различных отраслях хозяйства страны или региона. (Даже на небольших предприятиях ощущается потребность в информационной инфраструктуре, которая смогла бы обеспечить работу сотрудников в рамках единых информационных технологий.) Приведенный перечень и определяет потенциальное место работы выпускника этой новой специальности.

1. ЦЕЛИ И ЗАДАЧИ АДМИНИСТРИРОВАНИЯ ОБЪЕКТЫ АДМИНИСТРИРОВАНИЯ

Администрирование информационными системами – сложный процесс, основной целью которого является приведение информационной системы в соответствие целям и задачам предприятия или организации. Для достижения этой основной цели системное управление должно быть построено таким образом, чтобы минимизировать необходимое время и ресурсы, направляемые на управление системой и, в то же время, максимизировать доступность, производительность и продуктивность системы.

1.1.Обязанности системного администратора

В обязанности системного администратора входят:

· планирование системы;
· планирование нагрузки;
· установка и конфигурация аппаратных устройств;
· установка программного обеспечения;
· контроль защиты;
· архивирование (резервное копирование) информации;
· создание и управление счетами пользователей;
· определение и управление подсистемами;
· управление системными ресурсами;
· мониторинг производительности;
· управление лицензиями;
· документирование системной конфигурации и т.д.

1.2. Направления работы администраторов

Для снижения расходов на управление информационной системой и поддержку его качества обычно создают **три различные направления работы администраторов,** каждое из которых отвечает за определенные задачи управления и удовлетворение определенных потребностей пользователей.

1.2.1. Управление рабочими местами

Цель управления: обеспечить пользователей необходимыми вычислительными ресурсами.

Управление рабочими местами, как правило, включает в себя однообразную работу — установку и обновление приложений, перемещение пользователей и т. д. Из-за того, что пользователи могут находиться на значительном расстоянии, специалисты, выполняющие поддержку рабочих мест, пытаются решить максимальное количество проблем, не подходя к каждому рабочему месту в отдельности. Это создает потребность в средствах администрирования, которые хорошо работают в режиме удаленного доступа. Средства управления рабочим местом должны поддерживать широкий

диапазон настроек и служб рассылки, включая рассылку приложений, средства измерения и средства управления групповой политикой.

1.2.2. Управление центром обработки данных

Цель управления: обеспечить доступность служб и достоверность данных.

Специфика работы диспетчеров центра обработки данных заключается в поставке большим группам пользователей большого количества централизованно предоставляемых служб работы с приложениями. Отсюда весьма жесткие требования к надежности работы этих диспетчеров и к достоверности рассылаемых пользователям приложений

1.2.3.Управление сетью

Цель управления: обеспечить штатную работу сети.

Управление сетью имеет первоочередной задачей обеспечить передачу максимально возможного объема данных при хорошей достоверности, доступности и безопасности. Управление сетью в большей степени, чем центр обработки данных и управление рабочими местами, связано с текущим контролем состояния огромного числа сетевых устройств. На этом направлении весьма полезно использование диагностических средств контроля, которые предупреждают о возникновении проблем, автоматически фиксируя их по мере появления и выдавая при необходимости предупреждения.

1.3. Объекты администрирования

Под объектами администрирования понимают те компоненты системы, которые нуждаются во внимании со стороны администратора. В зависимости от направления работы администратора объектами администрирования могут быть как отдельные пользователи, так и их более крупные объединения, различные сетевые устройства, а также базы данных. Рассмотрим рабочие группы и сети как объекты администрирования.

1.3.1. Рабочая группа

Рабочая группа представляет собой логическое объединение компьютеров нескольких пользователей, чьи информационные потребности или деятельность взаимосвязаны, в результате чего возникает необходимость совместного использования файловых ресурсов. Обычно все компьютеры рабочей группы равноправны, в группе нет центрального компьютера, на котором сосредоточены ресурсы. Поэтому такая организация называется **одноранговой** сетью.

Сети рабочих групп существуют благодаря легкости установки и простоте обслуживания. Каждый пользователь сам управляет совместным доступом к ресурсам на своем компьютере, определяя, что будет предоставлено в общее пользование (принтер, устройство чтения компакт-дисков, жесткий диск или только отдельные файлы и каталоги) и у кого будет доступ к этому ресурсу. С

ростом сети появляются трудности- пользователей становится слишком много, соответственно возрастает количество совместно используемых ресурсов, возникают сложности с поиском нужного ресурса или с необходимостью установить разный режим доступа для разных членов рабочей группы.

Кроме того, неформальная структура рабочих групп означает отсутствие централизованного управления и администрирования. В большой рабочей группе затраты на поддержание ее работоспособности и администрирование становятся громадными, так как все действия по настройке приходится выполнять последовательно на всех компьютерах.

Для ограничения доступа используются пароли. Но с ростом одноранговой сети пароли множатся, запомнить их становится трудно, а сама система становится все более сложной. Пользователи, которым для доступа к различным ресурсам системы необходимо помнить множество паролей, начинают регулярно пользоваться одним и тем же паролем или выбирают такие, которые легко запомнить и, как следствие, легко угадать. Безопасность такой системы нарушается. Кроме того, если в системе используется удаленный доступ к сети и кто-то увольняется, переходя на работу в конкурирующую фирму, все пароли необходимо изменить, а это очень трудоемкий процесс. По этим причинам одноранговые сети непригодны для создания крупных сетей или сетей, требующих централизованного управления.

1.3.2. Доменная структура

Доменная структура предоставляет большую гибкость и упрощенный способ администрирования, который приемлем даже для самых крупных и сложных систем.

Домен – представляет собой группу компьютеров, использующих общую базу данных и общую политику безопасности. Домен включает в себя компьютер, выполняющий роль основного контроллера домена, хотя бы один компьютер, выполняющий роль резервного контроллера домена и, по крайней мере, одну рабочую станцию. В состав домена могут входить дополнительные резервные контроллеры домена, а также дополнительные серверы и рабочие станции.

Основной контроллер домена является самым важным компьютером домена. Он реализует политику безопасности домена и является основным местом хранения базы данных учетных записей.

Также можно сказать, что домен - это такая рабочая группа, в состав которой входит сервер. Она остается логическим объединением пользователей, которых связывают друг с другом не только провода, протянутые между компьютерами; другими словами - пользователей, совместно использующих общую информацию или занимающихся одним видом деятельности. Цель остается все той же: дать возможность членам группы совместно использовать информацию и таким образом облегчить им совместную работу и повысить производительность. Ключевым отличием является наличие в домене сервера,

что позволяет осуществлять администрирование и управление из единого центра.

Информационная система может состоять из одного домена или из нескольких связанных между собой доменов, как, например, корпоративная сеть, в которую входят тысячи отдельных рабочих станций, разбросанных по всему миру. В последнем случае отдельные рабочие станции объединяются в домены исходя из заданных требований доступа. Плюс концепции доменов состоит в том, что сеть легко расширяется или сужается, обеспечивая соответствующие модели доменов и различные их варианты и сочетания. Домены могут быть разделены на поддомены — произвольные имена, вводимые сетевым администратором для дальнейшего подразделения имени домена.

1.4. Преимущества модели доменов

Модель доменов обеспечивает следующие преимущества:

1 - гибкость при разработке конфигурации;
2 - централизованное администрирование сети;
3 - гибкость при добавлении новых пользователей и смене ограничений доступа;
4 - единая база данных учетных записей пользователей;
5 - объединенная система безопасности для всего домена;
6 - простота предоставления прав доступа к файлам и каталогам.

Последовательное администрирование всех компьютеров, которое необходимо выполнять в одноранговой сети, сильно ограничивает максимальный размер эффективной рабочей группы. В системе с доменами ограничения определяются только логической структурой организации. Вся компания целиком, даже крупная, может представлять собой один домен. В сети, организованной в виде домена, системный администратор может вносить в систему изменения с любого входящего в нее компьютера.

2. ИНСТАЛЯЦИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Цель построения всякой системы — достижение состояния, при котором все имеющиеся объекты управления будут находиться под контролем и готовы адекватно реагировать на управляющие воздействия.

2.1. Планирование информационной системы

- Перед установкой системы необходимо знать ответы на следующие вопросы:
- Какие задачи по обработке информации решает информационная система?
- Сколько и какие компьютеры используются в информационной системе?
- Как построена сеть (топология, маршрутизация и т.п.)?
- Какова политика безопасности в информационной системе? и т.д.

Развертывание новой сетевой структуры целесообразно начать с создания единственного домена, который легче всего администрировать, и по мере необходимости добавлять новые домены. При этом один домен может содержать несколько географически разнесенных и администрируемых индивидуально объектов – подразделений или организационных единиц.

Для создания нескольких доменов могут быть следующие причины:

- различные требования к безопасности для отдельных подразделений;
- очень большое количество объектов;
- различные Internet-имена для доменов;
- децентрализованное администрирование сети.

После того как разработана сетевая структура организации (т.е. создано несколько доменов или один с несколькими подразделениями и по ним распределены пользователи), следующий этап - продумать административную иерархию.

Если внутри домена создано дерево организационных единиц или подразделений, то обязанности администраторов отдельных подразделений можно распределить между определенными пользователями и группами. В этом случае уменьшается число сотрудников, которые получают полный контроль над всем доменом.

Этот процесс называется **делегированием прав администрирования**.

При модернизации устаревших систем, а также при добавлении к действующим вновь созданных объектов возникает проблема интеграции. Это означает соединение различных информационных систем в пределах одной организации или же различных организаций в одно целое. Различия в технологии и операционных системах могут сделать интеграцию очень

сложной. Стратегией для преодоления этих трудностей является одновременная разработка всей системы.

Для того чтобы в дальнейшем избежать отказов систем вследствие их недостаточной нагрузочной способности, а также для обеспечения надлежащей производительности компьютеров и емкости запоминающих устройств, следует оценить будущие потребности в их нагрузочной способности на основе прогноза. Этот прогноз должен учитывать требования к новым системам, а также текущие и прогнозируемые тенденции использования компьютеров и сетей.

2.2. Приемка систем

Необходимо задать критерии приемки новых систем и провести соответствующие испытания до их приемки. Для этого рассматриваются следующие пункты:

- требования к производительности и нагрузочной способности компьютеров;
- подготовка процедур восстановления и перезапуска систем после сбоев, а также планов действий в экстремальных ситуациях;
- подготовка и тестирование повседневных операционных процедур в соответствии с заданными стандартами;
- указание на то, что установка новой системы не будет иметь пагубных последствий для функционирующих систем, особенно в моменты пиковой нагрузки на процессоры (например, в конце месяца);
- подготовка персонала к использованию новых систем.

2.3.Учетные записи пользователей и группы

Создание учетных записей и групп занимает важное место в обеспечении безопасности информационной системы, поскольку, назначая им права доступа, администратор получает возможность ограничить пользователей в доступе к конфиденциальной информации компьютерной сети, разрешить или запретить им выполнение в сети определенного действия, например, архивацию данных или завершение работы компьютера. Каждый пользователь сети должен иметь в одном из доменов свою учетную запись. В учетную запись заносятся имя пользователя, пароль, различные ограничения на работу в сети.

Пользователей можно объединять в **локальные и глобальные группы**, имеющие единый набор разрешений и прав доступа. Объединение пользователей в группы позволяет изменять права доступа и разрешения для всей группы одновременно.

Например, в операционной системе Windows 2000 имеется ряд встроенных глобальных и локальных групп, на основе которых можно начинать работу по управлению правами пользователей сети. Локальная группа существует и сохраняет свои разрешения только в том домене, в котором она создана, в то

время как глобальная группа находится в одном из доменов, но сохраняет разрешения во всех доменах-доверителях.

Хорошо продуманная структура групп может сэкономить время на администрирование, а также предотвратить нежелательный доступ.

2.4. Имена доменов

У каждого компьютера в сети должно быть уникальное имя. Например – КОМ-1. Рекомендуется использовать не более 15 символов для имени компьютера. Если на компьютере планируется использовать выход в глобальную сеть Интернет и установлен сетевой протокол TCP/IP, то имя компьютера может содержать до 63 символов, включающих только числа 0-9, буквы A-Z, a-z и дефисы. Можно использовать и другие символы, но только если это не будет мешать другим пользователям найти компьютер в сети.

Компьютеры, имеющие непосредственный доступ в глобальную сеть, часто называют хост- компьютерами. Имя хост-узла - это имя, которое можно присвоить компьютеру для облегчения к нему доступа в сети IP.

Формат имени хост-узла с именами поддомена и домена:

[HostName].[SubdomainName].[DomainName]

Например, **КОМ-1.инф.com**

Имена домена и поддомена являются дополнительными дескрипторами компьютера.

2.5.Отношения доменов

В сети, состоящей из двух и более доменов, каждый домен действует как отдельная сеть со своей базой данных учетных записей. Однако даже в наиболее жестко структурированной организации некоторым пользователям из одного домена могут понадобиться какие-нибудь ресурсы из другого домена. Обычное решение этой проблемы, связанной с настройкой уровней доступа пользователей между различными доменами, называется установлением доверительных отношений.

2.5.1.Недоверительные отношения между доменами

Может существовать несколько доменов, между которыми не установлены доверительные отношения. Например, у пользователя могут быть учетные записи в каждом домене многодоменной сети. На рис.1 показана сеть с двумя доменами; один домен называется Финансы (Ф), а другой Маркетинг (М).

Когда пользователь регистрируется в домене М, он получает доступ к его ресурсам, как установлено администратором, но у него нет при этом доступа к домену Ф. Аналогично при входе в домен Ф у пользователя нет доступа к домену М. Чтобы снова добраться до ресурсов домена М, пользователь должен выйти из домена Ф и войти в домен М.

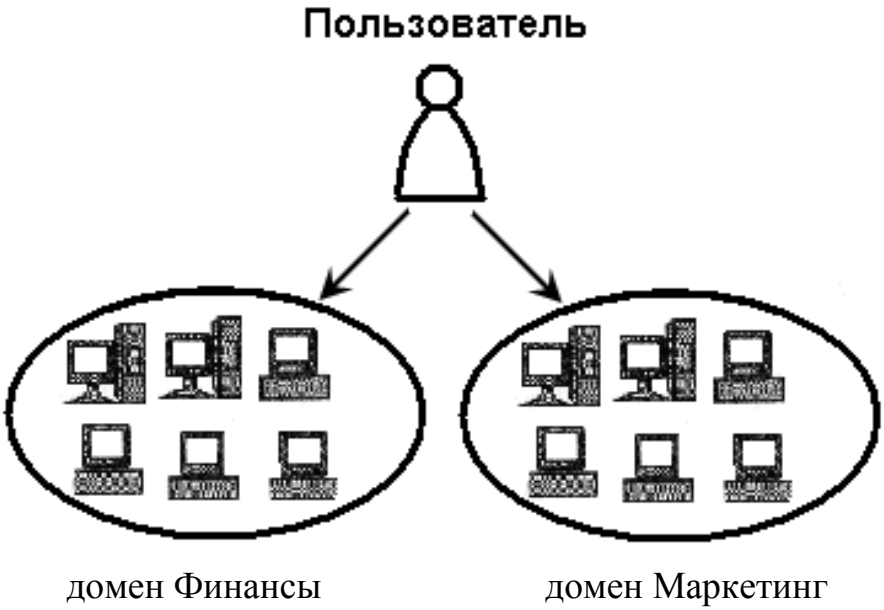

Рис.1. Домены, между которыми не установлены доверительные отношения

При таком подходе возникает проблема, когда пользователю, имеющему доступ к нескольким доменам, требуется одновременный доступ к их ресурсам, что при данной организации невозможно. Каждый раз, когда надо будет сменить пароль или изменить права доступа, администратору придется пройтись по доменам, регистрируясь и выполняя нужные изменения в каждом из них. Это очень трудоемкий процесс.

2.5.2. Односторонние доверительные отношения

Чтобы удовлетворить пользователя, которому необходим доступ к обоим доменам (М и Ф), описанным выше, можно установить между доменами одностороннее доверительное отношение. Рис. 2 иллюстрирует этот самый простой тип доверительных отношений. Домен Ф является доменом-доверителем, а М — доверенным доменом.

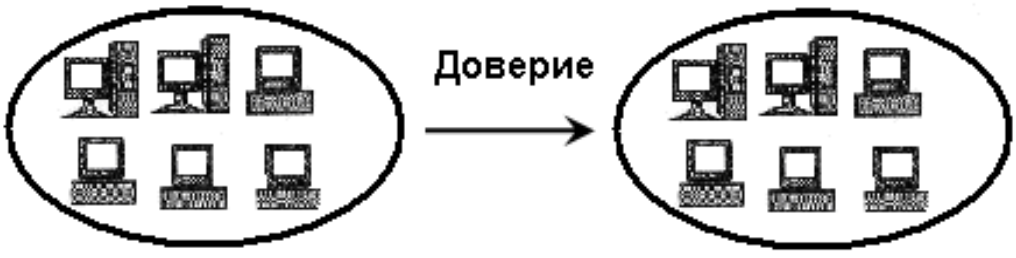

Рис.2. Одностороннее доверительное отношение

Если пользователь может войти в домен М, то домен Ф доверяет ему, считая, что пользователь вошел и в него. Это вовсе не означает, что пользователь автоматически получит доступ к ресурсам домена Ф; ему должны быть выданы соответствующие разрешения администратором этого домена. Это не означает также, что пользователи, которые вошли непосредственно в домен Ф, имеют доступ к домену М, доверенному домену.

Для того чтобы это стало возможным, необходимо отдельно установить еще одно одностороннее доверительное отношение, в котором доменом-доверителем будет М, а доверенным доменом — Ф.

2.5.3. Двусторонние доверительные отношения

Двусторонние доверительные отношения предоставляют большую гибкость регулирования доступа пользователя к ресурсам и значительно упрощают администрирование сети. При двусторонних доверительных отношениях пользователь, вошедший в один домен, будет считаться прошедшим проверку подлинности в другом домене. У пользователя в этом случае должен быть доступ к ресурсам другого домена в пределах, установленных администратором этого домена. Двусторонние доверительные отношения устанавливаются посредством двух односторонних доверительных отношений, по одному в каждом направлении, как показано на рис.3 .

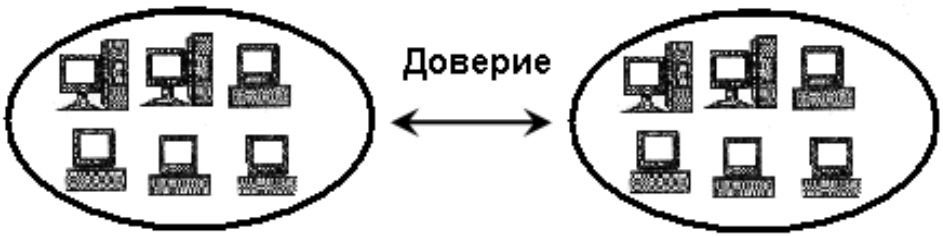

Рис. 3. Двусторонние доверительные отношения

Главным достоинством двусторонних доверительных отношений является то, что учетные записи пользователей необходимо создавать лишь один раз, предпочтительно в основном («домашнем») домене. Они будут доступны на всех доменах-доверителях, что значительно облегчает администрирование сети.

2.5.4.Непередаваемость доверия

Разрабатывая сеть, важно знать, что все доверительные отношения необходимо устанавливать по отдельности. Иначе говоря, доверие не передается из одного домена в другой. На рис.4 показана сеть из трех доменов. Домен М доверяет домену Ф, и наоборот. Третий домен, Образование (О),

имеет двусторонние доверительные отношения с доменом Ф. Однако домены О и М не будут доверять друг другу, пока между ними не будут установлены доверительные отношения.

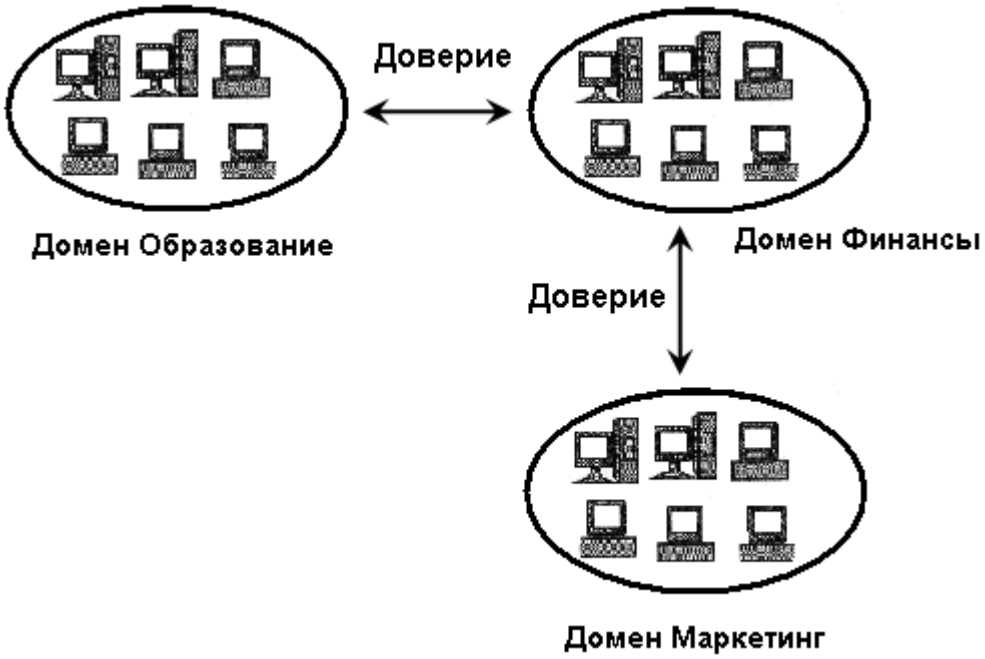

Рис.4. Несколько доменов с отдельно установленными доверительными отношениями

Если бы понадобилось предоставить пользователю из домена О доступ к ресурсам домена М или наоборот, то нужно было бы установить между этими доменами доверительные отношения, замкнув тем самым круг отношений.

Тогда диаграмма установленных отношений выглядела бы так, как показано на рис.5, если предположить, что устанавливаются двусторонние доверительные отношения.

2.6.Модели доменов

Существуют четыре модели структуры доверительных отношений между доменами. Это модели:

- с одним доменом;
- одним главным доменом;
- несколькими главными доменами;
- полностью доверительными отношениями.

Сеть может использовать одну из этих моделей, некую вариацию модели или сочетание двух и более моделей, используемых в различных частях сети. Но базовые кирпичики остаются теми же.

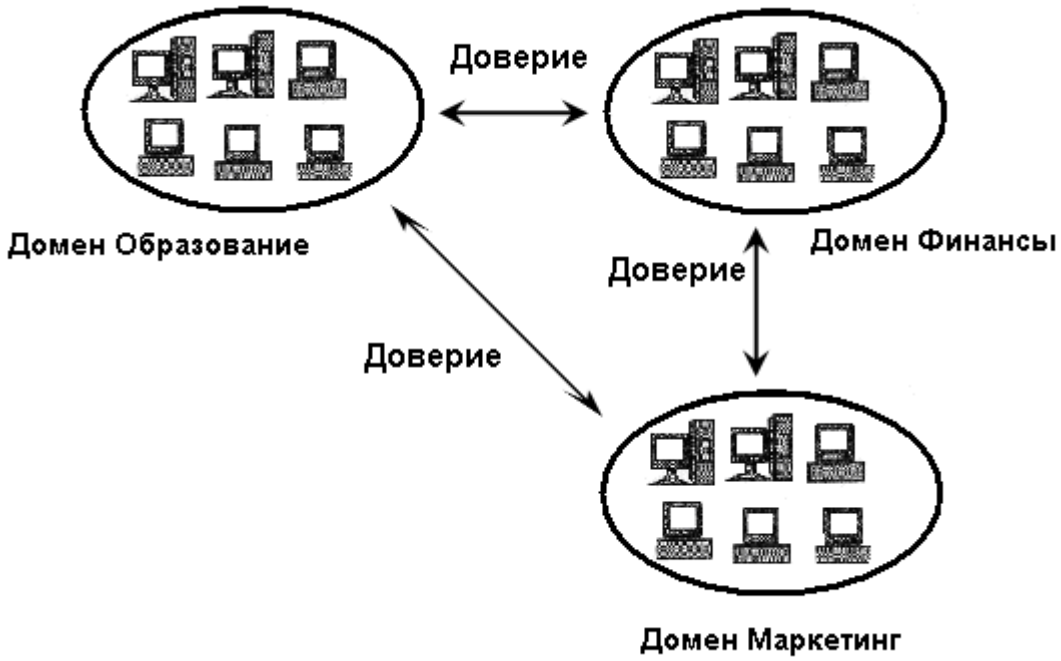

Рис.5. Несколько доменов с полным набором доверительных отношений

2.6.1. Модель с одним доменом

Это самая простая модель; все серверы и клиенты входят в один домен. Локальные и глобальные группы совпадают, а все администраторы могут администрировать все серверы. Поскольку домен один, нет нужды в доверительных отношениях.

Сеть с одним доменом является эффективной и полезной моделью для небольшого предприятия, где не так уж много серверов и пользователей. Модель с одним доменом не подходит, если:

- пользователи используют различные наборы ресурсов и имеют различные потребности;
- предприятие разрастается и отделы располагаются в нескольких зданиях, на разных этажах или вообще далеко друг от друга;
- время, затрачиваемое на просмотр ресурсов сети, огромно.

Преимущества модели с одним доменом	**Недостатки модели с одним доменом**
-Простота администрирования -Централизованное управление учетными записями пользователей -Отсутствие доверительных отношений и необходимости управлять ими -Локальные группы задаются только один раз	-Отсутствие группирования пользователей по подразделениям или другим признакам -Снижение производительности при увеличении числа ресурсов -Отсутствие логического группирования ресурсов -Время на просмотр ресурсов растет с увеличением числа серверов

2.6.2. Модель с одним главным доменом

Модель с одним главным доменом подходит для организации, в которой сравнительно мало пользователей и возможно логичное объединение ресурсов в группы, когда число ресурсов возрастает. Все учетные записи пользователей, а также глобальные группы создаются в главном домене. Но каждый домен подразделения может завести свои локальные группы. На рис.6 представлена структура модели с одним главным доменом.

Первейшей функцией главного домена является централизованное ведение учетных записей. Обязательно также наличие хотя бы одного резервного контроллера домена, так как база данных всех учетных записей пользователей хранится только на основном и резервных контроллерах главного домена. Все остальные домены (домены ресурсов) действуют в основном как распорядители ресурсов. У каждого из них имеется свой набор ресурсов, которые доступны во всей сети, но могут администрироваться на месте. Модель с одним главным доменом это естественное развитие модели с одним доменом. Однако эта модель перестает быть пригодной, если число пользователей становится слишком большим. Производительность значительно снижается, так как подлинность каждой учетной записи проверяет один главный домен.

Преимущества модели с одним главным доменом	**Недостатки модели с одним главным доменом**
-Централизованное управление учетными записями пользователей -Глобальные группы задаются только один раз -Управление ресурсами на уровне подразделений -Для каждого домена ресурса требуется установить только одностороннее доверительное отношение	-Снижение производительности при увеличении числа пользователей - Зависимость от надежности контроллеров главного домена - В каждом домене ресурсов требуется определять локальные группы

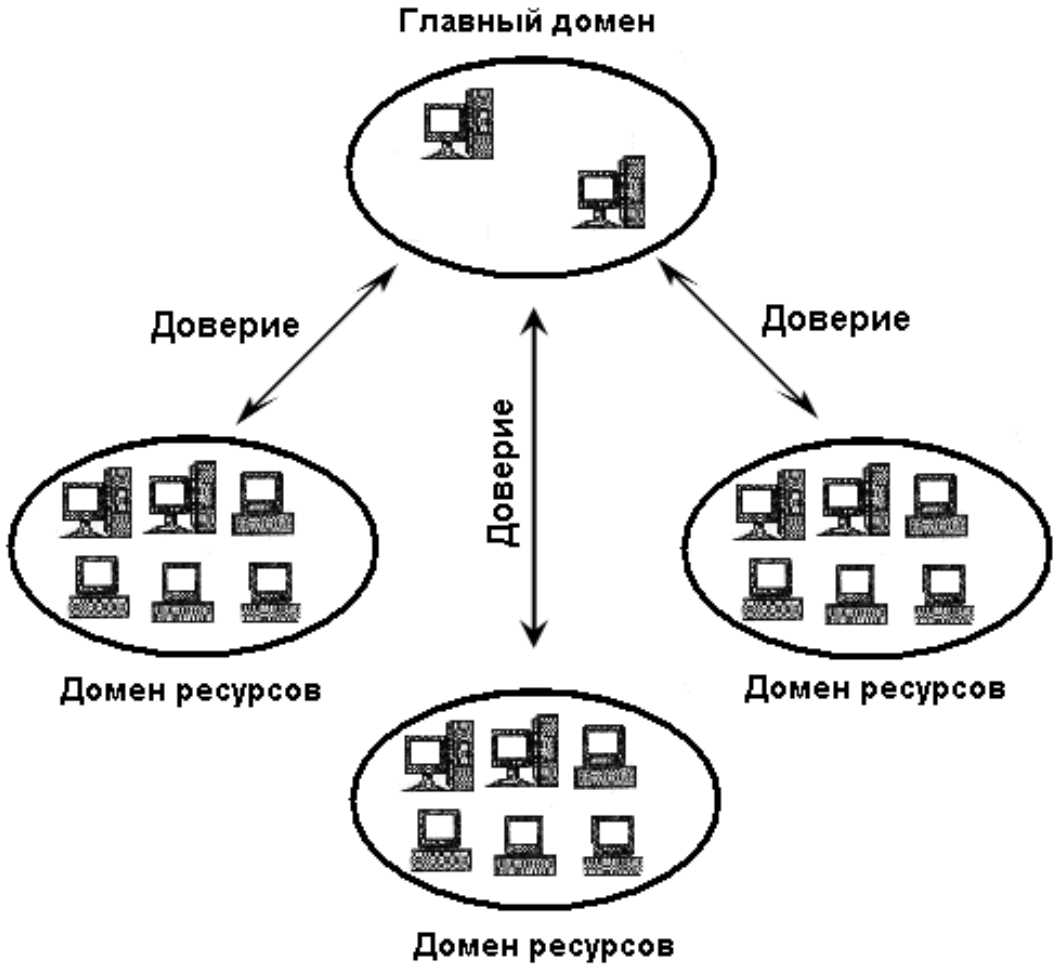

Рис. 6. Модель с одним главным доменом

2.6.3. Модель с несколькими главными доменами

Такая модель подходит для организаций с большим числом пользователей и централизованной структурой управления.

В ней обеспечивается централизованное администрирование двух и более главных доменов, а ресурсы распределены между доменами ресурсов (рис.7). В этой модели имеется небольшое число главных доменов, между которыми установлены двусторонние доверительные отношения. Учетные записи пользователей хранятся в главных доменах и распределены между ними сравнительно равномерно. Делить учетные записи пользователей между главными доменами можно исходя из логического объединения пользователей в группы или чисто формально, например, по именам в алфавитном порядке. Для каждого пользователя имеется только одна учетная запись в одном из главных доменов. Все домены ресурсов доверяют каждому главному домену, но наличие доверительных отношений между доменами ресурсов совсем не обязательно. Управление ресурсами, такими как принтеры и файлы, осуществляется на уровне доменов ресурсов.

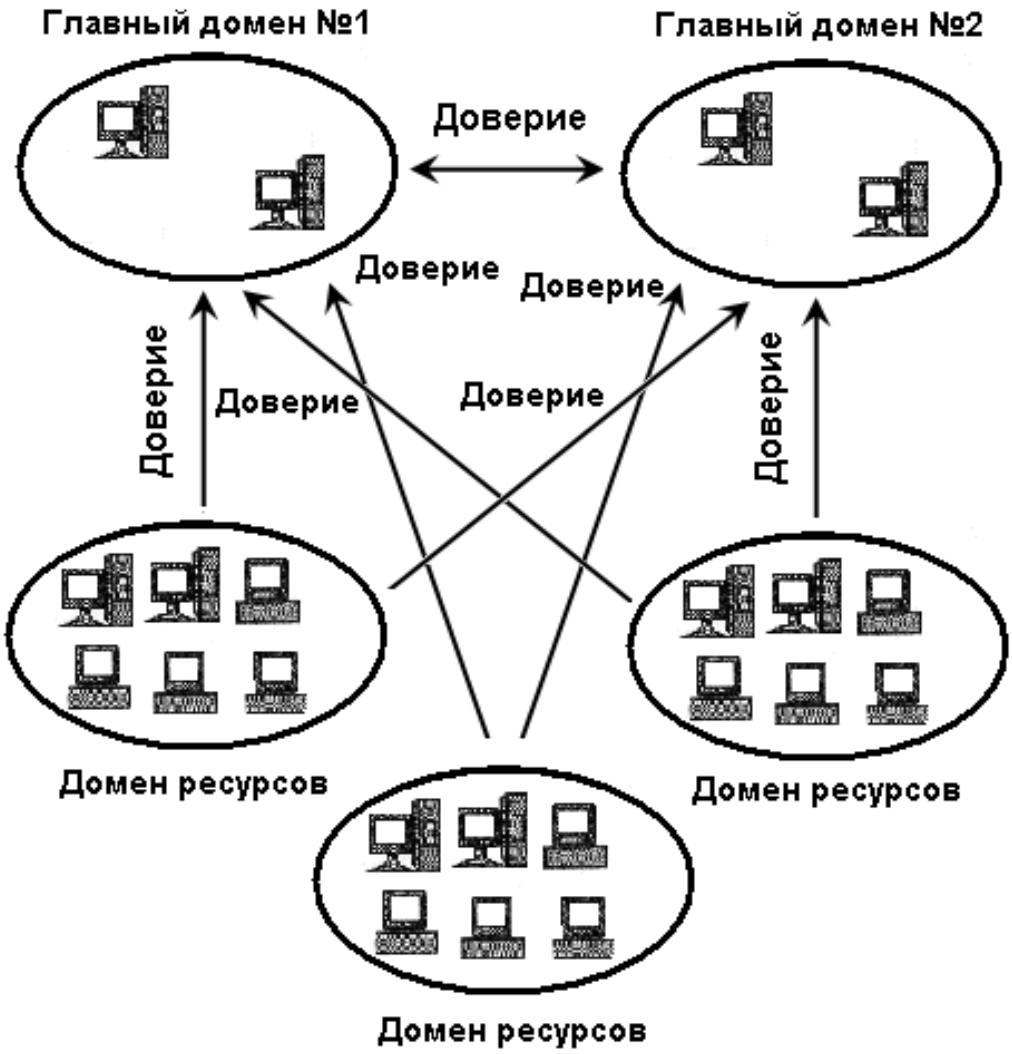

Рис. 7. Модель с несколькими главными доменами

Преимущества модели с несколькими главными доменами	**Недостатки модели с несколькими главными доменами**
- Централизованное управление учетными записями пользователей - Наращиваемость в соответствии с текущими требованиями -Управление ресурсами на уровне подразделений - Логическое объединение ресурсов	- Отсутствие единого места управления учетными записями пользователей и группами - Необходимость определять глобальные и локальные группы несколько раз и вносить в них изменения в нескольких местах - Возрастающая сложность доверительных отношений

2.6.4. Модель с несколькими главными доменами и полностью доверительными отношениями

Модель с несколькими главными доменами и полностью доверительными отношениями имеет смысл в относительно небольших организациях, которые переросли модель с одним доменом, но она не подходит для случая, когда доменов становится слишком много. У каждого домена должны быть установлены двусторонние доверительные отношения со всеми остальными доменами. Таким образом, число доверительных отношений растет экспоненциально с увеличением числа доменов. Число доверительных отношений, которые требуется установить в сети с п доменами, равно п*(п-1). Если у вас пять доменов, то понадобится двадцать доверительных отношений, добавление еще одного домена приведет к необходимости установить дополнительно десять доверительных отношений.

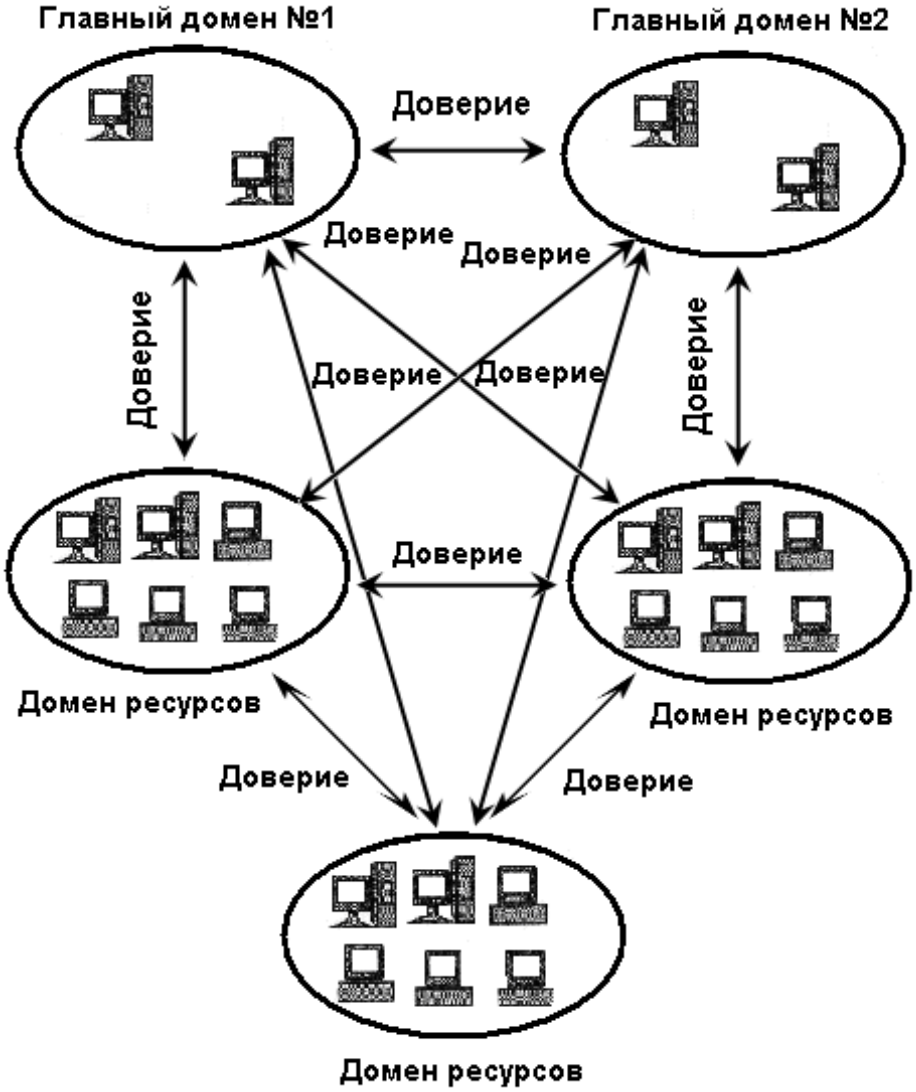

Рис. 8. Модель с несколькими главными доменами и полностью доверительными отношениям

Преимущества модели с несколькими главными доменами и полностью доверительными отношениями	**Недостатки модели с несколькими главными доменами и полностью доверительными отношениями**
-Логическое объединение в группы пользователей и ресурсов -Управление ресурсами на уровне подразделений - Наращиваемость в соответствии с текущими требованиями -Требуется полное взаимное доверие между администраторами всех доменов	- Отсутствие единого места управления учетными записями пользователей и группами - Необходимость определять глобальные и локальные группы несколько раз и вносить в них изменения в нескольких местах - Очень сложные доверительные отношения

3. ЗАДАЧИ АДМИНИСТРИРОВАНИЯ И ОСНОВНЫЕ СЛУЖБЫ

Независимо от объекта управления, желательно, чтобы при администрировании информационных систем (причем любого масштаба и независимо от формы организации – бумажной, полностью автоматизированной или смешанной) выполнялся ряд функций, которые определены международными стандартами, обобщающими опыт применения систем управления в различных областях. Существуют рекомендации ITU-T X.700 и близкий к ним стандарт ISO 7498-4, которые делят задачи управления на несколько функциональных групп:

- управление конфигурацией сети и изменениями,
- управление безопасностью,
- анализ качества ИС,
- учет работы и производительности сети.

Соответственно этим основным группам создаются службы администрирования.

3.1.Служба управления конфигурациями и изменениями

Управление конфигурациями определяется как процесс, с помощью которого администрация информационной системы может систематически идентифицировать, устанавливать связи, сопровождать и управлять различными компонентами системы. Этот процесс гарантирует целостность компонент и трассируемость всех изменений, возникающих в любой момент жизненного цикла системы.

Трассируемостью называется возможность идентифицировать и историю, и текущее состояние (статус) каждого объекта конфигурации в любой точке жизненного цикла.

Объектами конфигурации являются все основные результаты деятельности по разработке системы. Объекты конфигурации могут включать аппаратуру, программы, документацию, обучение и обслуживание. Объектам конфигурации могут быть присвоены номера для простоты прослеживаний.

Процесс управления конфигурациями состоит из следующих подпроцессов:

3.1.1. Идентификация конфигураций.
3.1.2. Контроль за конфигурациями.
3.1.3. Вычисление статуса конфигурации.
3.1.4. Аудиты/обзоры конфигураций.

3.1.1. Идентификация конфигураций

Процесс идентификации конфигураций требует выполнения следующих шагов:

- Определение объектов конфигурации.
- Выбор схемы наименования объектов конфигурации.

- Определение утверждаемых схем.
- Определение внутренних схем.

- ОПРЕДЕЛЕНИЕ ОБЪЕКТОВ КОНФИГУРАЦИИ

На начальном этапе следует определить, что входит в инфраструктуру системы и насколько подробно предполагается отслеживать ее отдельные элементы. Излишне высокая степень детализации позволяет при необходимости учесть даже минимальные возможности и отклонения, однако требует существенных ресурсов на ведение базы данных. Здесь, как и в других областях, должно работать простое правило: издержки, связанные с внедрением и эксплуатацией системы, не должны превышать положительного эффекта от ее внедрения.

Каждый объект системы, который может изменять свое представление, содержание, структуру или статус, подпадает под управление конфигурациями и, таким образом, должен быть определен с самого начала. Все имеющиеся конфигурационные единицы должны быть помечены соответствующими им учетными номерами.

- ВЫБОР СХЕМЫ НАИМЕНОВАНИЯ ОБЪЕКТОВ КОНФИГУРАЦИИ

Желательно, чтобы по учетному номеру можно было определить, к какому типу относится конфигурационная единица, какой она версии и т.д. Схема наименования, применяемая для учетных номеров, чаще всего включает следующие данные:

- тип объекта (например, документ или коды);
- имя объекта;
- идентификация программы или проекта;
- номер версии;
- номер ревизии (ревизия для конкретной версии);
- данные о готовности.

- ОПРЕДЕЛЕНИЕ УТВЕРЖДАЕМЫХ и ВНУТРЕННИХ СХЕМ

Во время жизненного цикла системы могут создаваться и использоваться внутренние и утверждающие схемы. Такие схемы обеспечивают моментальный снимок состояния системы в некоторый момент времени. Схема может быть представлена документом или набором документов. Моменты времени задаются администратором как точки инициализации контролирующих действий функции управления конфигурациями.

Реально полезной для компании является информация о конфигурационных единицах, хранение которой организовано в едином центральном хранилище, в соответствии с общими для всех типов конфигурационных единиц правилами и возможностью легкого и быстрого доступа к ней. Все остальные варианты обладают рядом недостатков:

сложностью получения необходимых данных, ограниченностью, сложностью поддержки и сопровождения, неадекватностью реальным потребностям бизнеса и т.д.

Семейство ОС Windows используют реестр - централизованную базу данных, в которой содержатся сведения о конфигурации и параметры всех версий Microsoft Windows. Реестр содержит информацию обо всех аппаратных средствах, программном обеспечении, операционной системе и сетевых параметрах компьютера. Эта сложная иерархическая база данных принимает участие во всех аспектах работы Windows 2000.

Для системных администраторов особенно важны: понимание принципов работы реестра, выполняемых им задач, а также умение манипулировать реестром, вопросы администрирования и защиты реестра, а также его резервного копирования и восстановления.

3.1.2. Контроль за конфигурациями

В работе любой организации или компании неизбежны изменения - новые условия деловой активности, появление новых аппаратных и программных средств, устаревание существующих систем и т. п., - которые требуют соответствующих мер со стороны администраторов информационных систем. Причины внесения изменения могут быть самыми разными: запросы пользователей, реакция на выявленную проблему, реакция на возникший инцидент, требования бизнеса.

Часто предлагаемые изменения инфраструктуры потенциально могут оказать существенно большее влияние на ее остальные элементы, нежели предполагалось изначально. Поэтому принятие решения об изменении должно осуществляться с учетом различной информации и при взаимодействии с другими процессами. Большая часть необходимой для принятия решения информации содержится в базе данных конфигурационных единиц. Для проведения стандартных изменений необходимо определить все потенциально связанные с изменением конфигурационные единицы, оценить влияние на них данного изменения, проверить, не ведет ли оно к снижению качества предоставляемых услуг, оценить экономическую эффективность изменения и в итоге принять его или отвергнуть.

Если изменение принимается, пересматриваются объекты конфигурации, их идентификационные номера, модифицируется схема, на которую изменение оказало влияние.

Последующий анализ произведенных изменений обязателен. В ходе такого анализа выясняется, удалось ли осуществить изменение, достигнут ли ожидаемый эффект, какие возникли сложности в ходе его осуществления и т.д. Иногда изменения могут не привести к ожидаемому результату и оказать неблагоприятное воздействие на работу различных систем и приложений. В этом случае следует вернуть все системы к состоянию, которое предшествовало

внесению изменения, поэтому рекомендуется заранее планировать процедуры возврата к предыдущему состоянию.

3.1.3. Вычисление статуса конфигураций

После того, как изменение объекта конфигурации санкционировано, должна возникнуть некоторая временная задержка на время реализации изменения. ВСК есть механизм, используемый для прослеживания эволюции каждого объекта системы и его текущего статуса. ВСК обеспечивает администратора большим количеством информации об объекте, включая то, как он разрабатывается и все ли требуемые свойства действительно реализованы. В конечном счете ВСК обеспечивает документацию о статусе каждого объекта конфигурации в любой момент процесса разработки.

Вычисление статуса как функция увеличивает свою сложность по мере развития разработки. Так как эта сложность в основном выражается в быстром росте объемов данных, которые записываются и обрабатываются, поэтому используются автоматические процессы, генерирующие отчеты о статусах.

3.1.4. Аудиты и обзоры конфигураций

Администраторы должны быть уверены, что требуемое управление конфигурацией реализуется - другими словами, все принятые изменения реализованы, а результат представляет собой то, что специфицировано в его проектной документации. Все это может обеспечиваться различными методами, но в любом случае рекомендуется организовывать регулярные аудиты и обзоры конфигурационного управления, проверки истинности хранящейся информации. Такие проверки не являются простыми и недорогими мероприятиями, поэтому их не делают частыми. Должны быть разработаны специальные процедуры, определяющие последовательность проведения проверок и необходимые для этих целей ресурсы.

Существенную помощь при организации такого рода проверок могут оказать специфичные средства автоматизированного управления различным оборудованием и приложениями.

Заключение

Процессы управления конфигурациями и изменениями — основа развертываемой системы управления инфраструктурой и предоставляемых ею услуг. В том или ином виде данные процессы уже реализованы на любом предприятии. В то же время, слабо реализованные процессы могут не только не улучшить качества управления инфраструктурой, но и привести к обратному эффекту путем предоставления неточной информации и внесения неконтролируемых изменений в компоненты инфраструктуры.

Положительный эффект от реализации процесса управления конфигурациями и изменениями выражается в следующем:

- эффективное планирование расходов, определение стоимости содержания инфраструктуры и отдельных ее элементов;
- повышение производительности труда пользователей за счет более качественного обслуживания и меньшего числа нарушений в нем;
- повышение производительности труда — за счет уменьшения числа незапланированных работ, связанных с восстановлением систем от сбоев;
- наличие доступной, полной и достоверной информации обо всем имеющемся оборудовании и ПО, а также связанной с ними документации;
- возможность контроля за ценными конфигурационными единицами, отслеживание их технического состояния и качества функционирования;
- строгое соблюдение правил лицензирования в отношении используемых программ, снижение риска появления в системах закладок, вирусов, выявление случаев использования запрещенного ПО;
- повышение готовности к устранению аварийных и иных непредвиденных ситуаций;
- меньшее число неудачных, подлежащих возврату в исходное состояние изменений;
- возможность контроля и осуществления необходимых изменений.

3.2. Служба управления безопасностью

3.2.1. Безопасность информационной системы

Безопасность информационной системы – свойство, заключающееся в способности системы обеспечить конфиденциальность и целостность информации, т.е. защиту информации от несанкционированного доступа с целью ее раскрытия, изменения или разрушения.

В соответствии с общепринятым современным подходом выделяют следующие аспекты информационной безопасности:

- **доступность** (возможность за приемлемое время получить требуемую информационную услугу);
- **целостность** (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);
- **конфиденциальность** (защита от несанкционированного ознакомления).

Главная цель мер, предпринимаемых на административном уровне, состоит в том, чтобы сформировать программу работ в области повышения доступности информационных сервисов и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя фактическое состояние дел.

Первым этапом выработки подобной программы является анализ угроз и рисков.

Все **угрозы информационным системам** можно объединить в обобщающие их три группы.

1. Угроза раскрытия — возможность того, что информация станет известной тому, кому не следовало бы ее знать.

2. Угроза целостности — умышленное несанкционированное изменение (модификация или удаление) данных, хранящихся в вычислительной системе или передаваемых из одной системы в другую.

3. Угроза отказа в обслуживании — возможность появления блокировки доступа к некоторому ресурсу вычислительной системы.

Выделяют следующие классы отказов:

1. Отказ пользователей – возникает по следующим причинам:

- нежелание работать с информационной системой;
- невозможность работать с системой в силу отсутствия соответствующей подготовки;
- невозможность работать с системой в силу отсутствия технической поддержки.

2. Внутренний отказ информационной системы– возникает по следующим причинам:

- отступление (случайное или умышленное) от установленных правил эксплуатации;
- ошибки при (пере)конфигурировании системы;
- отказы программного и аппаратного обеспечения;
- разрушение данных;
- разрушение или повреждение аппаратуры.

3. Отказ поддерживающей инфраструктуры– возникает по следующим причинам:

- нарушение работы (случайное или умышленное) систем связи, электропитания, водоснабжения, кондиционирования;
- разрушение или повреждение помещений;
- невозможность или нежелание выполнения обслуживающим персоналом и/или пользователями своих обязанностей (гражданские беспорядки, аварии на транспорте, террористический акт или его угроза, забастовка и т.п.).

3.2.2. Средства обеспечения информационной безопасности

Средства обеспечения информационной безопасности в зависимости от способа их реализации можно разделить на следующие классы методов:

- аппаратные методы, реализующие физическую защиту системы от несанкционированного доступа, аппаратные функции идентификации

периферийных терминалов системы и пользователей, режимы подключения сетевых компонентов и т. д.

К техническим средствам физической защиты информации (ЗИ) относят механические, электронно-механические, электромеханические, оптические, акустические, лазерные, радио и радиционные и другие устройства, системы и сооружения, предназначенные для создания физических препятствий на пути к защищаемой информации и способные выполнять самостоятельно или в комплексе с другими средствами функции защиты информации.

- **организационные методы** подразумевают рациональное конфигурирование, организацию и администрирование системы. В первую очередь это касается сетевых информационных систем, их операционных систем, полномочий сетевого администратора, набора обязательных инструкций, определяющих порядок доступа и работы в сети пользователей;

- **технологические методы**, включающие в себя технологии выполнения сетевого администрирования, мониторинга и аудита безопасности информационных ресурсов, ведения электронных журналов регистрации пользователей, фильтрации и антивирусной обработки поступающей информации;

- **программные методы** - это самые распространенные методы защиты информации (например, программы идентификации пользователей, парольной защиты и проверки полномочий, брандмауэры, криптопротоколы и т. д.). Без использования программной составляющей практически невыполнимы никакие, в том числе и первые три группы методов (то есть в чистом виде организационные, технологические и аппаратные методы защиты, как правило, реализованы быть не могут — все они содержат программный компонент).

3.2.3. Типы защиты сети

Типы защиты сети можно разбить на четыре основные категории:

- физическая безопасность;
- защита пользователей;
- защита файлов;
- защита от вторжения извне.

Физическая безопасность

Любому компьютеру, является ли он сервером в сети, рабочей станцией, ноутбуком или общедоступным терминалом в уличном киоске, необходимо обеспечить физическую защиту.

Защита пользователя

У защиты пользователя есть два аспекта:

- - предоставление пользователю доступа к тем ресурсам, в которых он нуждается;

- - не предоставлять (и даже не показывать) пользователю те ресурсы, которые ему не требуются для работы. К таким ресурсам относятся наиболее конфиденциальная информация компании и личные данные пользователей.

Управление доступом сводится к взаимному опознанию пользователя и системы и установлению факта допустимости использования ресурсов конкретным пользователем в соответствии с его запросом.

Защита файлов

При обеспечении защиты файлов также имеется два аспекта:

- управление доступом к файлу;
- защита целостности файла.

Нарушитель, преднамеренно проникнувший в систему, может извлечь, изменить или уничтожить информацию в файлах. Поэтому необходим ввод некоторых ограничений на обработку файлов, содержащих важную информацию.

Защита от вторжения извне

Защита реализуется процедурами идентификации, установления подлинности и регистрации обращений.

Идентификация и подтверждение подлинности могут осуществляться в процессе работы неоднократно, чтобы исключить возможность входа в систему нарушителя, выдающего себя за истинного пользователя.

3.2.4. Модели администрирования сети и способы обеспечения безопасности

Администрирование сети можно организовать одним из четырех основных способов:

- централизованно на всем предприятии;
- по отделам или группам («распределенное» администрирование);
- по операционным системам;
- в виде сочетания предыдущих способов.

Модели администрирования небольших и крупных, сложных систем могут совпадать. Они будут отличаться масштабами, но не по сути.

Централизованное администрирование

В модели с централизованным администрированием один человек, группа или отдел занимается администрированием всей сети организации, ее пользователей и ресурсов. Главным и очень серьезным недостатком централизованной схемы является ее недостаточная масштабируемость и

отсутствие отказоустойчивости. Производительность центрального компьютера всегда будет ограничителем количества пользователей, работающих с данным приложением, а отказ центрального компьютера приводит к прекращению работы всех пользователей.

Эта модель хорошо подходит небольшим и средним организациям, но может оказаться медленной и неэффективной для крупного или географически разбросанного предприятия. Однако с точки зрения безопасности централизованное администрирование является наилучшим. Оно гарантирует, что системная политика и процедуры являются однообразными для всей организации.

Распределенное администрирование

При распределенном администрировании управление сетью осуществляется на уровне отдела или рабочей группы. Хотя администрирование на этом уровне может быстро откликаться на нужды пользователей, часто это достигается за счет безопасности сети. При наличии нескольких администраторов политика администрирования в разных рабочих группах будет отличаться. Чем больше групп имеется в системе, тем больше доверительных отношений им требуется, что повышает возможность того, что в систему проникнет злоумышленник и воспользуется этими доверительными отношениями, чтобы добраться до совершенно секретной информации.

Администрирование по операционным системам

Когда администрирование домена производится по операционным системам, средства обеспечения безопасности значительно различаются в зависимости от используемых операционных систем. Например, если имеется свой администратор у сервера Windows NT Server, свой — у сервера Novell Net Ware и свой — у систем UNIX, то администратор каждой системы будет сам обеспечивать ее безопасность. Однако потребуется кто-то, кто будет разрешать различия во мнениях администраторов в случае возникновения проблем.

Смешанная модель администрирования

Смешанная модель администрирования сочетает элементы централизованной и распределенной моделей. Центральный администратор (или группа) гарантирует проведение политики безопасности на всем предприятии, а администраторы на уровне отделов или рабочих групп выполняют повседневную работу. При этом обычно требуется больше затрат на штат, чем может себе позволить небольшая организация, поэтому применение смешанной модели администрирования, как правило, ограничивается крупными предприятиями.

3.2.5. Заключение

Политика безопасности должна исполняться во всей организации.

Соответствие самому строгому уровню безопасности вместе с применением множества средств обеспечения безопасности при условии, что система неаккуратно спроектирована и плохо управляется, может привести к неэффективности защиты и сложности использования системы по её прямому назначению. Необходимо помнить, что практически всегда повышение уровня безопасности системы требует увеличения времени и усилий администратора на управление им.

При построении системы защиты разумно придерживаться следующих принципов:

Актуальность. Защищаться следует от реальных атак, а не от фантастических или же архаичных.

Разумность затрат. Поскольку 100% защиты обеспечить нереально, необходимо найти тот рубеж, за которым дальнейшие траты на повышение безопасности превысят стоимость той информации, которую может украсть злоумышленник.

3.3. Качество информационной системы

Качество информационной системы — это совокупность свойств системы, обусловливающих возможность ее использования для удовлетворения определенных в соответствии с ее назначением потребностей. Количественные характеристики этих свойств определяются показателями, которые необходимо контролировать и учитывать. Основными показателями качества информационных систем являются надежность, достоверность, безопасность (см. выше), эффективность.

3.3.1. Надежность

Это- свойство системы сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения.

Надежность - важнейшая характеристика качества любой системы, поэтому разработана специальная теория - теория надежности.

Теория надежности может быть определена как научная дисциплина, изучающая закономерности, которых следует придерживаться при разработке и эксплуатации систем для обеспечения оптимального уровня их надежности с минимальными затратами ресурсов.

Надежность - комплексное свойство системы; оно включает в себя более простые свойства, такие как безотказность, ремонтопригодность, долговечность и т д.

Безотказность - свойство системы сохранять работоспособное состояние в течение некоторого времени или наработки (наработка - продолжительность или объем работы системы).

Ремонтопригодность - свойство системы, заключающееся в приспособленности к предупреждению и обнаружению причин возникновения

отказов, повреждений и поддержанию и восстановлению работоспособного состояния путем проведения технического обслуживания и ремонтов.

Долговечность - свойство системы сохранять при установленной системе технического обслуживания и ремонта работоспособное состояние до наступления предельного состояния, то есть такого момента, когда дальнейшее использование системы по назначению недопустимо или нецелесообразно.

Показатель надежности — это количественная характеристика одного или нескольких свойств, определяющих надежность системы. В основе большинства показателей надежности лежат оценки наработки системы, то есть продолжительности или объема работы, выполненной системой. Показатель надежности, относящийся к одному из свойств надежности, называется единичным. Комплексный показатель надежности характеризует несколько свойств, определяющих надежность системы.

На сегодняшний день разработано много конкретных практических способов повышения надежности информационных систем.

Для обеспечения надежности технических средств чаще всего выполняется:

1) резервирование (дублирование) технических средств (компьютеров и их компонентов, сегментов сетей и т. д.);
2) использование стандартных протоколов работы устройств ИС;
3) применение специализированных технических средств защиты информации.

Для обеспечения надежности функционирования программного комплекса ИС выполняется:

1) тщательное тестирование программ, опытное исполнение программы с целью обнаружения в ней ошибок (обязательное условие эффективного тестирования - по крайней мере один раз выполнить все разветвления программы в каждом из возможных направлений);
2) использование стандартных протоколов, интерфейсов, библиотек процедур, лицензионных программных продуктов;
3) использование структурных методов для обеспечения надежной работы программных комплексов (иерархическое построение программ, разбиение программ на сравнительно независимые модули и т. д.);
4) изоляция параллельно работающих процессов, в результате чего ошибки в работе одной программы не влияют на работу операционной системы и других программ.

Надежность информационных систем не самоцель, а средство обеспечения своевременной и достоверной информации на ее выходе. Поэтому показатель достоверности функционирования имеет для информационных систем главенствующее значение.

3.3.2. Достоверность

Достоверность функционирования — свойство системы, обусловливающее безошибочность производимых ею преобразований информации. Достоверность функционирования информационной системы полностью определяется и измеряется достоверностью ее результатной информации.

Достоверность информации — это свойство информации отражать реально существующие объекты с необходимой точностью. Достоверность информации измеряется вероятностью того, что отражаемое информацией значение параметра отличается от истинного значения этого параметра в пределах необходимой точности.

Одним из наиболее действенных средств обеспечения достоверности информации в ИС является ее контроль. Контроль — процесс получения и обработки информации с целью оценки соответствия фактического состояния объекта предъявляемым к нему требованиям и выработки соответствующего управляющего решения.

Методы контроля достоверности информации, применяемые в ИС, весьма разнообразны. Классификация методов контроля может быть выполнена по большему числу признаков, в частности: по назначению, по уровню исследования информации, по способу реализации, по степени выявления и коррекции ошибок.

1. Классификация методов контроля достоверности по назначению

Профилактический контроль и одна из наиболее распространенных его форм — тестовый контроль, предназначены для выявления состояния системы в целом и отдельных ее звеньев до включения системы в рабочий режим. Целью профилактического контроля, осуществляемого часто в утяжеленном режиме работы системы, является выявление и прогнозирование неисправностей в ее работе с последующим их устранением.

Рабочий контроль, или контроль в рабочем режиме, выполняется в процессе выполнения системой возложенных на нее функций. Он, в свою очередь, может быть разделен на функциональный контроль и контроль качества продукции. Функциональный контроль может преследовать цель либо только проверки работоспособности (отсутствия неисправностей) системы, либо, кроме того, установления места и причины неисправности (диагностический контроль). Контроль качества продукции является контролем достоверности информации как одного из важнейших показателей качества продукции выпускаемой ИС.

Генезисный контроль проводится для выяснения технического состояния системы в прошлые моменты времени с целью определения причин сбоев и отказов системы, имевших место в прошлом; сбора статистических данных об ошибках, их характере, величине и последствиях (экономических потерях) этих ошибок для ИС.

2. Классификация методов контроля достоверности по уровню исследования информации

Синтаксический контроль — это, по существу, контроль достоверности данных, не затрагивающий содержательного, смыслового аспекта информации. Предметом синтаксического контроля являются отдельные символы, реквизиты, показатели: допустимость их наличия, допустимость их кодовой структуры, взаимных сочетаний и порядка следования.

Семантический контроль оценивает смысловое содержание информации, ее логичность, непротиворечивость, согласованность, диапазон возможных значений параметров, отражаемых информацией, динамику их изменения.

Прагматический контроль определяет потребительную стоимость (полезность, ценность) информации для управления, своевременность и актуальность информации, ее полноту и доступность.

3. Классификация методов контроля достоверности по способу реализации

Организационный контроль достоверности является одним из основных в ИС. Он представляет собой комплекс мероприятий, предназначенных для выявления ошибок на всех этапах участия эргатического звена в работе системы, причем обязательным элементом этих мероприятий является человек или коллектив людей.

Программный контроль основан на использовании специальных программ и логических методов проверки достоверности информации или правильности работы отдельных компонентов системы и всей системы в целом. Программный контроль, в свою очередь, подразделяется на программно-логический, алгоритмический и тестовый.

Программно-логический контроль базируется на использовании синтаксической или семантической избыточности; алгоритмический контроль использует как основу вспомогательный усеченный алгоритм преобразования информации, логически связанный с основным рабочим алгоритмом.

Аппаратный контроль реализуется посредством специально встроенных в систему дополнительных технических схем. Этот вид контроля также подразделяется на непрерывный и оперативный (аппаратно-логический) контроль достоверности, а также непрерывный контроль работоспособности.

4. Классификация методов контроля достоверности по степени выявления и коррекции ошибок

Обнаруживающий фиксирует только сам факт наличия или отсутствия ошибки.

Локализующий позволяет определить как факт наличия, так и место ошибки (например, символ, реквизит и т. д.).

Исправляющий выполняет функции и обнаружения, и локализации, и исправления ошибки.

3.3.3. Эффективность

Это свойство системы выполнять поставленную цель в заданных условиях использования и с определенным качеством. Показатели эффективности характеризуют степень приспособленности системы к выполнению поставленных перед нею задач и являются обобщающими показателями оптимальности функционирования ИС, зависящими от локальных показателей, каковыми являются надежность, достоверность, безопасность.

Кардинальным обобщающим показателем является экономическая эффективность системы, характеризующая целесообразность произведенных на создание и функционирование системы затрат.

3.4. Учет работы и производительности сети

Управление производительностью включает в себя учет ресурсов, контролирование времени реакции, доступности, утилизации и компонентной задержки, а также регулировку, отслеживание и управление производительностью.

Путем анализа данных управления производительностью и учетом ресурсов администраторы могут определять, будут ли удовлетворены задачи производительности сети.

Проблема оптимизации работы информационной системы достигается путем решения нескольких задач: оптимизации клиентской части, оптимизации серверной части, снижения сетевого трафика.

Конечными узлами сети являются компьютеры и от их производительности и надежности во многом зависят характеристики всей сети в целом. Оптимизация компьютера включает две достаточно независимые задачи:

во-первых, выбор таких параметров конфигурации программного и аппаратного обеспечения, которые бы обеспечивали оптимальные показатели производительности и надежности этого компьютера как отдельного элемента сети;

во-вторых, выбор таких параметров протоколов, установленных в данном компьютере, которые бы гарантировали эффективную и надежную работу коммуникационных средств сети.

Окончательной проверкой ценности информационной системы является то, как и в какой степени она может быть задействована. Системы должны иметь такие характеристики, как простота, легкий доступ и достаточный уровень технологии.

4. АУДИТ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Под термином аудит Информационной Системы понимается системный процесс получения и оценки объективных данных о текущем состоянии ИС, действиях и событиях, происходящих в ней, устанавливающий уровень их соответствия определенному критерию.

В настоящее время актуальность аудита резко возросла, это обусловлено следующими причинами:

- увеличение зависимости организаций от информации и ИС;
- при модернизации и внедрении новых технологий их потенциал полностью не реализуется;
- возросла уязвимость ИС за счет повышения сложности элементов этой ИС, увеличения строк кода программного обеспечения, новых технологий передачи и хранения данных;
- расширился спектр угроз ИС;
- аудит ИС позволяет добиться максимальной отдачи от средств, инвестируемых в создание и обслуживание ИС.

Подход к проведению аудита ИС, как отдельной самостоятельной услуги, с течением времени упорядочился и стандартизировался. Крупные и средние аудиторские компании образовали ассоциации — союзы профессионалов в области аудита ИС, которые занимаются созданием и сопровождением стандартов аудиторской деятельности в сфере ИТ.

Ассоциация ISACA, занимающаяся открытой стандартизацией аудита ИС, основана в 1969 году и в настоящее время объединяет около 20 тысяч членов из более чем 100 стран, в том числе и России. Ассоциация координирует деятельность более чем 12 тыс. аудиторов информационных систем.

Основная декларируемая цель ассоциации — это исследование, разработка, публикация и продвижение стандартизованного набора документов по управлению информационной технологией для ежедневного использования администраторами и аудиторами информационных систем. В помощь профессиональным аудиторам и администраторам ассоциацией ISACA был разработан стандарт CoBiT (рис.9).

CoBiT — **К**онтрольные **ОБ**ъекты **И**нформационной **Т**ехнологии — открытый стандарт, первое издание вышло в 1996 году. Стандарт связывает информационные технологии и действия аудиторов, объединяет и согласовывает многие другие стандарты в единый ресурс, позволяющий авторитетно, на современном уровне получить представление и управлять целями и задачами, решаемыми ИС. CoBiT учитывает все особенности информационных систем любого масштаба и сложности. Применение стандарта CoBiT возможно как для проведения аудита ИС организации, так и для изначального проектирования ИС.

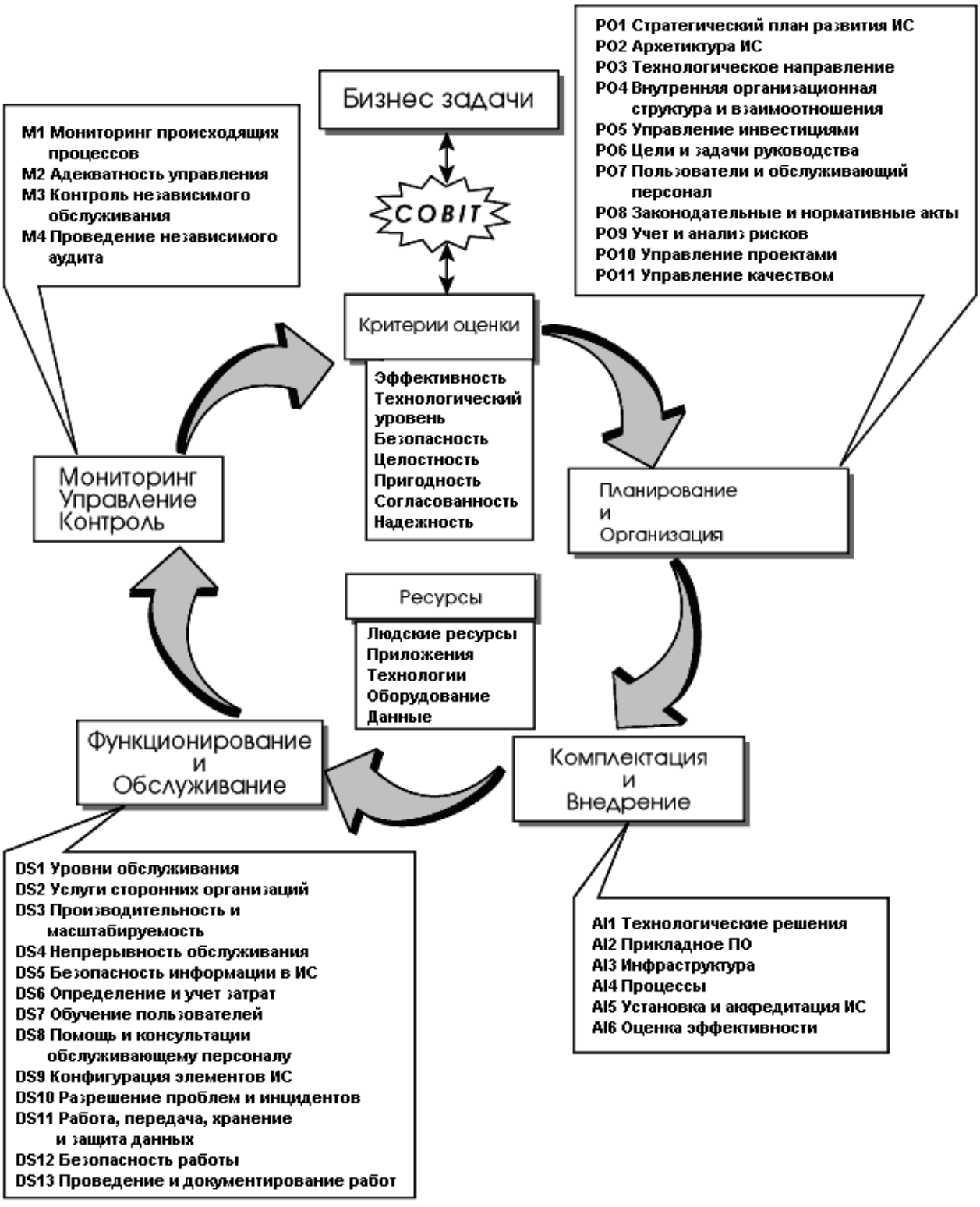

Рис. 9. Структура стандарта CoBIT

Бизнес-процессы (в верхней части схемы) предъявляют свои требования к ресурсам ИС, которые анализируются с использованием критериев оценки CoBiT на всех этапах построения и проведения аудита.

Четыре базовые группы содержат в себе тридцать четыре подгруппы, которые, в свою очередь, состоят из трехсот двух объектов контроля. Объекты контроля предоставляют аудитору всю достоверную и актуальную информацию о текущем состоянии ИС.

Преимущества CoBiT это его достаточность, масштабируемость и наращиваемость. CoBiT позволяет использовать любые разработки производителей аппаратно-программного обеспечения и анализировать полученные данные, не изменяя общие подходы и собственную структуру.

Результаты проведения аудита ИС организации можно разделить на три основных группы:

- организационные — планирование, управление, документооборот функционирования ИС;
- технические — сбои, неисправности, оптимизация работы элементов ИС, непрерывное обслуживание, создание инфраструктуры и т.дю;
- методологические — подходы к решению проблемных ситуаций, управлению и контролю, общая упорядоченность и структуризация.

Проведенный аудит позволит обоснованно создать следующие документы:

- Долгосрочный план развития ИС.
- Политика безопасности ИС организации.
- Методология работы и доводки ИС организации.
- План восстановления ИС в чрезвычайной ситуации.

5. АППАРАТНО-ПРОГРАММНЫЕ ПЛАТФОРМЫ АДМИНИСТРИРОВАНИЯ

Программное и аппаратное обеспечение в компьютере работают в неразрывной связи и взаимодействии. Состав программного обеспечения информационной системы называется программной конфигурацией.

5.1. Классификация служебных программных средств

Диспетчеры файлов. С их помощью выполняется большинство операций по обслуживанию файловой структуры: копирование, перемещение, переименование файлов, создание каталогов (папок), уничтожение объектов, поиск файлов и навигация в файловой структуре.

Средства сжатия данных (архиваторы). Предназначены для создания архивов.

Средства диагностики. Предназначены для автоматизации процессов диагностики программного и аппаратного обеспечения.

Программы инсталляции (установки). Предназначены для контроля за добавлением в текущую программную конфигурацию нового программного обеспечения.

Средства коммуникации. Разрешают устанавливать соединение с удаленными компьютерами, передают сообщения электронной почты, пересылают факсимильные сообщения и т.п..

Средства просмотра и воспроизведения.

Средства компьютерной безопасности. К ним относятся средства пассивной и активной защиты данных от повреждения, несанкционированного доступа, просмотра и изменения данных. Средства пассивной защиты - это служебные программы, предназначенные для резервного копирования. Средства активной защиты применяют антивирусное программное обеспечение.

5.2.Защита от вредоносного программного обеспечения

Компьютерный вирус - это небольшая программа, способная к саморазмножению и выполнению разных деструктивных действий. На сегодняшний день известно свыше 50 тыс. компьютерных вирусов.

Условно их можно классифицировать следующим образом:

1) **загрузочные вирусы** или BOOT-вирусы заражают boot-секторы дисков. Очень опасные, могут привести к полной потере всей информации, хранящейся на диске;
2) **файловые вирусы** заражают файлы. Делятся:
    - **на вирусы, заражающие программы** (файлы с расширением .EXE и .COM);
    - **макровирусы** - вирусы, заражающие файлы данных, например, документы Word или рабочие книги Excel;

- **вирусы-спутники** используют имена других файлов;
- **вирусы семейства DIR** искажают системную информацию о файловых структурах;

3) **загрузочно-файловые вирусы** способные поражать как код boot-секторов, так и код файлов;
4) **вирусы-невидимки** или **STEALTH-вирусы** фальсифицируют информацию прочитанную из диска так, что программа, какой предназначена эта информация получает неверные данные.
5) **ретровирусы** заражают антивирусные программы, стараясь уничтожить их или сделать нетрудоспособными;
6) **вирусы-черви**.

К общим средствам, помогающим предотвратить заражение и его разрушительных последствий, относят:

- резервное копирование информации (создание копий файлов и системных областей жестких дисков);
- избежание пользования случайными и неизвестными программами.
- перезагрузку компьютера перед началом работы, в частности, в случае, если за этим компьютером работали другие пользователи;
- ограничение доступа к информации, в частности, физическая защита дискеты во время копирования файлов с нее.

К программным средствам защиты относят разные антивирусные программы (антивирусы).

Антивирус - это программа, выявляющая и обезвреживающая компьютерные вирусы. Много современных антивирусных пакетов имеют в своем составе специальный программный модуль, называемый эвристическим анализатором, который способен исследовать содержимое файлов на наличие кода, характерного для компьютерных вирусов. Это дает возможность своевременно выявлять и предупреждать об опасности заражения новым вирусом.

Различают такие типы антивирусных программ:

1. **Программы-детекторы** предназначены для нахождения зараженных файлов одним из известных вирусов.
2. **Программы-лекари**. Лечение программы состоит в изъятии из зараженной программы тела вируса.
3. **Программы-ревизоры.** Эти программы запоминают данные о состоянии программы и системных областей дисков в нормальном состоянии (до заражения) и сравнивают эти данные в процессе работы компьютера. В случае несоответствия данных выводится сообщение о возможности заражения.

4. **Лекари-ревизоры** предназначены для выявления изменений в файлах и системных областях дисков и, в случае изменений, возвращают их в начальное состояние.
5. **Программы-фильтры** предназначены для перехвата обращений к операционной системе.
6. **Программы-вакцины** используются для обработки файлов и boot-секторов с целью предупреждения заражения известными вирусами (в последнее время этот метод используется все чаще).

Администраторы информационных систем должны быть всегда готовы к опасности проникновения вредоносного программного обеспечения в системы и по необходимости принимать специальные меры по предотвращению или обнаружению его внедрения. Предотвращение вирусов лучше, чем ликвидация последствий от их проникновения. В основе защиты от вирусов должны лежать хорошие знания и понимание правил безопасности, надлежащие средства управления доступом к системам.

5.3. Меры обеспечения безотказности ИС

Для аппаратного и программного обеспечения ИС можно рекомендовать следующие меры обеспечения безотказности:

- Ориентация на апробированные продукты известных компаний.
- Ориентация на надежных поставщиков, способных квалифицированно произвести установку, наладку и ввод в эксплуатацию новых продуктов, обучение и консультирование пользователей и обслуживающего персонала.
- Принятие решения о разработке и внедрении регламентов эксплуатации всех компонентов ИС, унификация регламентов.
- Унификация программных и аппаратных конфигураций, в том числе клиентских.

6 ЭКСПЛУАТАЦИЯ, СОПРОВОЖДЕНИЕ И ОБСЛУЖИВАНИЕ ИС

6.1. Процедуры по обслуживанию ИС

Цель: обеспечить целостность и доступность информационных сервисов.

Существует великое множество обязательных для исполнения ежедневных операций. Например, проверка правильности функционирования электронной почты и телеконференций, просмотр регистрационных файлов на предмет наличия ранних признаков неисправностей, контроль за подключением локальных сетей и за наличием системных ресурсов. Рассмотрим некоторые из них.

6.1.1.Резервное копирование данных

На сегодняшний день разработано множество способов, программ и устройств, предназначенных для защиты данных от потери, но в основе их лежит общий принцип — запись и хранение избыточной информации. В большинстве случаев он реализуется путем создания копий данных.

Различают два основных способа копирования данных:

- резервное копирование,
- архивирование.

Резервное копирование чаще всего планируется на ежедневной основе. Избыточные копии могут использоваться для восстановления в случае, если оригинальные файлы потеряны или повреждены.

Архивирование обычно выполняется над данными, ассоциированными с конкретным проектом, а не с системой в целом. В отличие от резервного копирования, пользователи обычно сами инициируют процесс архивирования данных по мере необходимости, поэтому наличие общей для всей сети политики архивирования часто неразумно.

Процедуру резервного копирования можно автоматизировать, но системный администратор обязан убедиться в том, что резервное копирование выполнено правильно и в соответствии с графиком. Практически любая сетевая операционная система содержит механизмы для создания резервных копий или зеркального ведения дисков. В большинстве случаев информация, хранящаяся в компьютерах, стоит дороже самих компьютеров. Кроме того, ее гораздо труднее восстановить.

При правильном подходе создание резервных копий данных позволяет администратору восстанавливать файловую систему (или любую ее часть) в том состоянии, в котором она находилась на момент последнего снятия резервных копий.

6.1.2.Ведение журналов регистрации событий

Операторы компьютеров должны вести журнал регистрации всех выполняемых заданий. Этот журнал должен по необходимости включать:

- время запуска и останова систем;
- подтверждение корректного оперирования с файлами данных и выходной информацией от компьютеров.

В журнал регистрации следует заносить зафиксированные пользователями сбои, касающиеся проблем с компьютерными и коммуникационными системами.

В связи с появлением проблемы (как сбойной ситуации) выделяют несколько областей:

Определение проблемы. - Выявляется проблема и выполняются шаги, необходимые для начала диагностики проблемы. Назначение этой области - изолировать проблему в конкретной подсистеме, например, в каком-нибудь аппаратном устройстве, программном изделии, компоненте микрокода или сегменте носителя.

Диагноз проблемы. - Определяется точная причина проблемы и воздействие, необходимое для решения этой проблемы.

Обход проблемы и восстановление. - Осуществляются попытки обойти проблему либо частично, либо полностью. Обычно эта операция является временной.

Решение проблемы. - Включает усилия, необходимые для устранения проблемы, которые должны быть занесены в график; например, это может быть замена отказавшего дисковода.

Отслеживание и управление проблемой. - Отслеживается проблема до ее полного решения. В частности, если для решения проблемы необходимо внешнее воздействие, то жизненно важная информация, описывающая эту проблему (такая, как информация контролирования состояния и отчеты о состоянии проблемы), включается в запись управления проблемой, которая вводится в базу данных этой проблемы.

6.1.3.Слежение за окружающей средой

Для определения условий, которые могут неблагоприятно сказаться на работе компьютерного оборудования и для принятия корректирующих мер, необходимо постоянно следить за окружающей средой, в том числе за влажностью, температурой и качеством источников электропитания.

6.1.4.Оперирование с носителями информации и их защита

Цель: предотвратить повреждение информационных ресурсов и перебои в работе организации. Следует определить надлежащие операционные процедуры для защиты компьютерных носителей информации (магнитные ленты, диски, кассеты), входных/выходных данных и системной документации от повреждения, похищения и несанкционированного доступа.

6.1.5.Обмен данными и программами

Цель: предотвратить потери, модификацию и несанкционированное использование данных.

Обмены данными и программами между организациями необходимо контролировать. Такие обмены следует осуществлять на основе формальных соглашений. Должны быть установлены процедуры и стандарты для защиты носителей информации во время их транспортировки. Необходимо учитывать последствия для производственной деятельности и системы безопасности от использования электронного обмена данными и сообщениями электронной почты, а также требования к средствам управления безопасностью.

6.1.6.Рекомендации для аудита

Осуществлять аудит (ревизию) не рекомендуется при обычном функционировании системы. Но рекомендуется, чтобы каждый администратор системы знал, как использовать подсистему аудита. В частности необходимо знать, как запускать, останавливать, и просматривать основную контрольную информацию. Администратор будет нуждаться в этих функциях, если он подозревает, что его система атакована.

6.1.7.Квотирование дискового пространства

Администрирование больших компьютерных сетей, где серверы поддерживают работу сотен пользователей, сопряжено с рядом сложностей. Одна из них - учет дискового пространства сервера, занятого файлами сотрудников компании.

Подобная проблема просто решается с помощью введения квот на дисковое пространство, доступное для работы каждому пользователю. Например, в Windows 2000 администратор может квотировать дисковое пространство по каждому тому и для каждого пользователя.

После установки квот дискового пространства пользователь сможет хранить на томе ограниченный объем данных, в то время как на этом томе может оставаться свободное пространство

Планирование перехода на аварийный режим

Аварийное резервное оборудование предоставляет возможность временного продолжения обработки данных в случае повреждения или отказа основного оборудования. Администраторы компьютеров и сетей должны подготовить соответствующий план перехода на аварийный режим для каждого информационного сервиса.

Аварийное резервное оборудование и процедуры перехода на аварийный режим необходимо регулярно тестировать.

Управление и обслуживание программных и технических средств.

1. Подключение и удаление аппаратных средств.

Любая компьютерная сеть состоит из трех основных компонентов:

- активное оборудование (концентраторы, коммутаторы, сетевые адаптеры и др.);
- коммуникационные каналы (кабели, разъемы);
- сетевая операционная система.

Естественно, все эти компоненты должны работать согласованно. Для корректной работы устройств в сети требуется их правильно инсталлировать и установить рабочие параметры.

В случае приобретения новых аппаратных средств или подключения уже имеющихся аппаратных средств к другой машине систему нужно сконфигурировать таким образом, чтобы она распознала и использовала эти средства.

Изменение конфигурации может быть как простой задачей (например, подключение принтера), так и более сложной (подключение нового диска).

Для того чтобы принять правильное решение о модернизации системы, как системному администратору, необходимо проанализировать производительность системы.

Плохая производительность обычно является следствием того, что одно из устройств требует намного больше ресурсов, чем остальные. Чтобы исправить положение, вы должны выявить устройство, которое расходует максимальную часть времени при выполнении задачи. Такое устройство называется у*зким местом*

Определение узкого места — критический этап в процессе улучшения производительности.

2. Инсталляция новых программных средств

После приобретения нового программного обеспечения его нужно инсталлировать и протестировать. Если программы работают нормально, необходимо сообщить пользователям об их наличии и местонахождении.

Как правило, самой ответственной и самой сложной задачей системного администратора являются инсталляция и конфигурирование операционной системы, т.к. от правильности действий зависит загруженность администратора.

После инсталляции и оптимальной настройки операционной системы начинается процесс установки программного обеспечения. И здесь на первый план выходят проблемы совместимости различных программ, а при установке серверного программного обеспечения, — еще и безопасности.

3. Ведение локальной документации

Системный администратор должен документировать все инсталлируемые программные средства, не входящие в стандартный пакет поставки,

документировать разводку кабелей, вести записи по обслуживанию всех аппаратных средств, регистрировать состояние резервных копий и документировать правила работы с системой.

Также следует учитывать, что система учета, ядро, различные утилиты — все эти программы выдают данные, которые регистрируются и в конце попадают на диски. Эти данные тоже являются локальной документацией, характеризующей работу конкретной системы. Однако срок полезной службы большинства данных ограничен, поэтому их нужно обобщать, упаковывать и наконец, выбрасывать.

Операционные системы и аппаратные средства, на которых они работают, время от времени выходят из строя. Задача администратора — диагностировать сбои в системе и в случае необходимости вызвать специалистов. Как правило, найти неисправность бывает намного сложнее, чем устранить ее.

6.2.Средства мониторинга и анализа

Все многообразие средств, применяемых для мониторинга и анализа вычислительных сетей, можно разделить на несколько крупных классов:

Системы управления сетью — централизованные программные системы, которые собирают данные о состоянии узлов и коммуникационных устройств сети, а также данные о трафике, циркулирующем в сети. Эти системы не только осуществляют мониторинг и анализ сети, но и выполняют в автоматическом или полуавтоматическом режиме действия по управлению сетью — включение и отключение портов устройств, изменение параметров мостов адресных таблиц мостов, коммутаторов и маршрутизаторов и т.п.

Средства управления системой. Средства управления системой часто выполняют функции, аналогичные функциям систем управления, но по отношению к другим объектам. В первом случае объектами управления являются программное и аппаратное обеспечение компьютеров сети, а во втором — коммуникационное оборудование. Вместе с тем некоторые функции этих двух видов систем управления могут дублироваться, например средства управления системой могут выполнять простейший анализ сетевого трафика.

Встроенные системы диагностики и управления. Эти системы выполняются в виде программно-аппаратных модулей, устанавливаемых в коммуникационное оборудование, а также в виде программных модулей, встроенных в операционные системы. Они выполняют функции диагностики и управления единственным устройством, и в этом их основное отличие от централизованных систем управления.

Анализаторы протоколов. Представляют собой программные или аппаратно-программные системы, которые ограничиваются, в отличие от систем управления, лишь функциями мониторинга и анализа трафика в сетях.

Оборудование для диагностики и сертификации кабельных систем. Условно это оборудование можно поделить на четыре

основные группы: сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры (мультиметры).

Экспертные системы. Этот вид систем аккумулирует человеческие знания о выявлении причин аномальной работы сетей и возможных способах приведения сети в работоспособное состояние. Экспертные системы часто реализуются в виде отдельных подсистем различных средств мониторинга и анализа сетей: систем управления сетями, анализаторов протоколов, сетевых анализаторов.

Многофункциональные устройства анализа и диагностики. Приборы, совмещающие функции нескольких устройств: анализаторов протоколов, кабельных сканеров и даже ряд возможностей ПО сетевого управления.

7. АДМИНИСТРИРОВАНИЕ БАЗ ДАННЫХ

Администратор - лицо, ответственное за целостность и непротиворечивость данных в системе, безопасность системы, эффективность функционирования системы и использования ею ресурсов. СУБД (система управления баз данных) "видит" администратора как пользователя, обладающего определенным набором привилегий. Привилегии администратора дают ему возможность использовать такие команды и утилиты СУБД и иметь доступ к таким системным таблицам, которые недоступны рядовым пользователям. Как правило, СУБД предоставляют в распоряжение администратора еще и специальный инструментарий, который обеспечивает удобный интерфейс для выполнения функций администратора.

Во всех СУБД различаются (хотя и называются по-разному) два уровня администрирования: системный администратор (администратор СУБД) и администраторы базы данных (БД). Одна копия программного продукта СУБД может поддерживать одновременное существование многих БД - коллекций данных и прикладных средств их обработки. Разные БД могут быть связаны с разными проектами и даже с разными организациями, поэтому у каждой БД должен быть свой администратор. Функции системного администратора относятся ко всей системе в целом, его права и привилегии распространяются на все объекты и на всех субъектов в системе. Функции администратора БД относятся не только к подмножеству системных ресурсов, выделенных конкретной БД, его права и привилегии распространяются на объекты, относящиеся к данной БД, и на субъектов, имеющих к ним доступ.

Руководства для разных СУБД по-разному формулируют функции администратора, но в конечном итоге они сводятся к следующим:

- инсталляция СУБД;
- управление памятью;
- управление разделением данных между пользователями;
- копирование и восстановление БД;
- управление безопасностью в системе;
- передача данных между СУБД и другими системами;
- управление производительностью.

Инсталляция СУБД является функцией только системного администратора.

Данные в СУБД хранятся на внешней памяти. Администратор должен обеспечить такое выделение памяти, чтобы с одной стороны, ее было достаточно для хранения и эффективного доступа к данным, а с другой - минимальное количество выделенной памяти оставалось неиспользованным.

Разделение данных между пользователями при их параллельной работе обеспечивается автоматически средствами СУБД и поддерживается средствами языка SQL. Однако при одновременной работе независимых приложений

(иногда - и в рамках одного приложения) могут возникать конфликты одновременного доступа. Администратор, имея исчерпывающее представление о дисциплинах разделения, применяемых СУБД, выступает в роли консультанта прикладных программистов, сводя к минимуму взаимное блокирование приложениями друг друга.

Копирование и восстановление являются необходимыми для гарантирования сохранности данных даже при полном крахе системы. Эта часть функций администратора включает в себя работу с соответствующими утилитами СУБД и с протоколами транзакций.

Управление безопасностью данных защищает их от несанкционированных пользователей. Оно состоит в регистрации пользователей в системе, выделении пользователям привилегий и бюджетов.

Данные, хранящиеся в БД, могут потребоваться для использования в других БД, работающих в другой инсталляции, или в приложениях, не зависящих от СУБД. Для целей переноса данных в распоряжении администрации имеются утилиты выгрузки данных в формате, пригодном для переноса и, соответственно, загрузки данных, поступивших из другой системы.

Управление производительностью включает в себя три аспекта: настройку параметров функционирования самой СУБД, отдельных БД и отдельных приложений. Первое обеспечивается конфигурированием системы и использованием системных утилит. Второе - составом и структурой компонентов БД (таблиц, индексов, триггеров и т.п.), третье - выбором средств разработки и оптимизацией формулировок запросов, т.е. зависит в основном от прикладного программиста.

ПРИМЕЧАНИЕ

Назначение IP адресов при администрировании крупных сетей

Класс	Первые биты	Наименьший номер сети	Наибольший номер сети	Максимальное число узлов в сети
A	0	1.0.0.0	126.0.0.0	2^{24}
B	10	128.0.0.0	191.255.0.0	2^{16}
C	110	192.0.1.0	223.255.255.0	2^{8}
D	1110	224.0.0.0	239.255.255.255	Multicast
E	11110	240.255.255.255	247.255.255.255	Зарезервирован

В протоколе IP существует несколько соглашений об особой интерпретации IP-адресов:

- Если весь IP-адрес состоит только из двоичных нулей, то он обозначает адрес того узла, который сгенерировал этот пакет; этот режим используется только в некоторых сообщениях ICMP.
- Если в поле номера сети стоят только нули, то по умолчанию считается, что узел назначения принадлежит той же самой сети, что и узел, который отправил пакет.
- Если все двоичные разряды IP-адреса равны 1, то пакет с таким адресом назначения должен рассылаться всем узлам, находящимся в той же сети, что и источник этого пакета. Такая рассылка называется *ограниченным широковещательным сообщением (limited broadcast).*

Если в поле номера узла назначения стоят только единицы, то пакет, имеющий такой адрес, рассылается всем узлам сети с заданным номером сети. Например, пакет с адресом 192.190.21.255 доставляется всем узлам сети 192.190.21.0. Такая рассылка называется *широковещательным сообщением (broadcast).*

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1. Администрирование сети Microsorft Windows NT: учебный курс/ пер. с англ. — М.: Издательский отдел «Русская редакция» ТОО «Channel Trading Ltd.». — 1997. — 496с.: ил.
2. Олифер Н.А., Олифер В.Г. Администрирование и настройка ОС WINDOWS NT / Центр Информационных Технологий, 1998, http://www.citforum.ru/
3. Сетевые средства Microsoft Windows NT Server 4.0 / пер. с англ. — СПб.: — BHV — Санкт-Петербург, 1997.
4. Ресурсы Microsoft Windows NT Server 4.0. Книга l / перев. с англ. — СПб.: — BHV — Санкт-Петербург, 1997.
5. Сети предприятий на основе Windows NT для профессионалов. Стерн, Монти / пер». с англ. — СПб.: Питер, 1999.

ОГЛАВЛЕНИЕ

Учебное издание

Алаева Светлана Станиславовна

Ситанов Сергей Вячеславович

Бобков Сергей Петрович

Администрирование
в информационных сетях

Учебное пособие

Техн. редактор В.Л. Родичева

Подписано в печать 17.02.2010. Формат 60×84$^{1}/_{16}$. Бумага писчая.
Усл. печ. л. 3,02. Уч.-изд. л. 3,35. Тираж 50 экз. Заказ
ГОУ ВПО Ивановский государственный химико-технологический университет
Отпечатано на полиграфическом оборудовании кафедры экономики и финансов
ГОУ ВПО «ИГХТУ»
153000, г. Иваново, пр. Ф. Энгельса, 7